

Contents

I	Theory and Practice	3
1	Divisibility	5
1.1	Definitions and Propositions	5
1.1.1	Divisibility by Certain Numbers	11
1.2	gcd and lcm	17
1.3	Numeral Systems	22
1.3.1	Introduction	22
1.3.2	Base Conversion	24
1.3.3	Logarithms	28
1.3.4	Number of Digits	31
1.4	Some Useful Facts	33
1.5	Solved Problems	41
1.6	Exercises	51
2	Modular Arithmetic	55
2.1	Basic Modular Arithmetic	55
2.2	Modular exponentiation	61
2.3	Residue Systems	64
2.4	Bézout's Lemma	68
2.4.1	Bézout's Identity and Its Generalization	68
2.4.2	Modular Arithmetic Multiplicative Inverse	71
2.5	Chinese Remainder Theorem	73
2.6	Wilson's Theorem	78
2.7	Euler's and Fermat's Theorem	80
2.8	Quadratic Residues	83
2.8.1	Euler's Criterion	87
2.8.2	Quadratic Reciprocity	92
2.8.3	Jacobi Symbol	93
2.9	Wolstenholme's Theorem	95
2.10	Lucas' Theorem	103
2.11	Lagrange's Theorem	106
2.12	Order, Primitive Roots	111
2.13	Carmichael Function	123
2.13.1	Primitive λ -Root	126
2.14	Pseudoprimes	126
2.14.1	Fermat Pseudoprimes and Carmichael Numbers	127

2.15	Using Congruence in Diophantine Equations	130
2.15.1	Some Useful Properties	130
2.16	Exercises	136
3	Arithmetic Functions	145
3.1	Definitions	145
3.2	Floor and Ceiling	148
3.2.1	Fractions and Increasing Functions	153
3.2.2	Power of a Prime in a Number	154
3.2.3	Kummer's Theorem	156
3.3	Common Arithmetic Functions	159
3.3.1	Number of Divisors	159
3.3.2	Sum of Divisors	162
3.3.3	Euler's and Jordan's Totient Functions	163
3.4	Characterizing Multiplicative Functions	167
3.5	Dirichlet Product and Mobius Inversion	169
3.6	More on Multiplicative Functions	174
3.6.1	More on τ	179
3.6.2	More on σ and its Generalization	184
3.6.3	More on $\varphi(n)$ and $J_k(n)$	190
3.7	Menon's Identity	198
3.8	Liouville Function	201
3.9	Exercises	205
4	Primes	213
4.1	Introduction	213
4.2	Infinitude Of Primes	215
4.3	Formula For Primes	222
4.4	Bertrand's Postulate and A Proof	225
4.5	Miscellaneous	233
4.6	Distribution of Prime Numbers	237
4.6.1	Chebyshev Functions	238
4.7	The Selberg Identity	245
4.8	Primality Testing	248
4.8.1	Primality Testing for Famous Classes of Primes	252
4.9	Prime Factorization	256
4.9.1	Fermat's Method of Factorization	258
4.9.2	Pollard's Rho Factorization	258
4.10	Exercises	262
4.11	Open Questions In Primes	263
5	Special Topics	267
5.1	Thue's Lemma	267
5.2	Chicken McNugget Theorem	272
5.3	Vietta Jumping	276
5.4	Exponent gcd Lemma	280

5.5	A Congruence Lemma Involving gcd	281
5.6	Lifting the Exponent Lemma	284
5.6.1	Two Important and Useful Lemmas	285
5.6.2	Main Result	285
5.6.3	The Case $p = 2$	287
5.6.4	Summary	288
5.6.5	Solved Problems	289
5.7	Zsigmondy's Theorem	291
5.8	How to Use Matrix?	295
5.8.1	Proving Fibonacci Number Identities	301
5.9	A Proof for Law of Quadratic Reciprocity	303
5.10	Darij-Wolstenholme Theorem	307
5.11	Generalization of Wilson's and Lucas' Theorem	313
5.12	Inverse of Euler's Totient Function	315
5.13	Exercises	320

Glossary

A	Identities and Well-Known Theorems	331
II	Problem Column	337
6	Solving Challenge Problems	339
7	Practice Challenge Problems	369